DR SOLOMON'S CASE BOOK

The computer virus has wrought havoc worldwide since it first struck in 1989. Dr Alan Solomon dons his white coat to probe the history of computer vandalism and recommend some treatment.

In The Beginning...

It all began in March 1988. In my capacity as a PC troubleshooter, I was rescuing data from damaged disks when I was told of an unusual problem. A number of a customer's floppy disks were giving '(c) Brain' as a volume label, and he suspected it was a virus. We examined the disks, and found about 3K of code that could transfer itself from floppy to floppy without the user realising what was happening.

If a machine was accidentally booted from one of these disks, you'd get the 'Not a system disk' message. But by then the program had reserved a chunk of memory for itself. Thereafter, any access to a 360K floppy disk would also result in this code copying itself to the new floppy, if it wasn't already there.

I had heard rumours about such a phenomenon, but considered it 'theoretically possible, but not yet seen'. Now I knew the threat was real, that it was here in Britain, and that the infections don't necessarily work via COMMAND.COM, as was commonly believed. They were named 'Computer Viruses', because of the analogy with the biological kind.

It was such an interesting, annoying and potentially damaging phenomenon, that my colleagues and me decided that people must be warned. The reaction surprised us. The response to a technical article is normally a few letters of appreciation, one of which may pick up on a particular point. But the report on the Brain virus incited mass disbelief.

At that time, the idea was very new. Many people had been misinformed about viruses, and my article contradicted most of that. There was even one pundit who declared he could prove viruses were theoretically impossible. Sadly, we never asked to see the proof.

Ever since, the whole virus scene has been characterised by this surprising surge of emotion. What ought to be a PC technical subject about as interesting as the inner workings of the BIOS (Basic Input/Output System) is blown up into a field in which passions rage, and fear, uncertainty and doubt pervade.

On the Second Day...

In May 1988, we were sent a copy of the 'Italian' virus. This infected hard disks as well as floppies ('Brain' only infects 360K disks).

Around then, we started seeing reports of a hard disk version of 'Brain'. But the internal structure of this virus means it is unlikely, and after three years no-one has come forward with a specimen. This was probably the first of many non-existent viruses, which are believed in but can never be killed. How do you prove the non-existence of something? How do you write a detector for it?

Mis-information from articles and books is another ever-present problem with viruses. In many situations, accurate information is outvoted by an erroneous report that is widely copied, making the information it carries appear to come from multiple sources. This is a dangerous problem that can lead people into taking actions which are not useful and may be counter-productive.

In July 1988, the 'Stoned' virus turned up (see *What is a Virus?*). This has become one of the most successful viruses in the world. It infects hard and floppy disks, but unlike 'Brain' and 'Italian', it rarely announces itself. It came from New Zealand, and on one in eight infective boot-ups, it announces 'Your PC is now Stoned!'. In one local variant, it announces 'Your WC is now flooded'.

Searching for a Solution

The main defence of any virus, is to be inconspicuous. If you spot it, you'll swat it. So like a mouse, the virus survives not being noticed. If you know you have mice you get a cat. Keeping a cat is usually simple – you just need cat food and tin openers. Anti-virus software should be as easy. To make a cat catch a mouse, you just let go of it, and it knows the rest.

When I began searching for the solution, I made my first foreign contact in August 1988. Austrian-based Herr Swoboda had read some of my reports, and sent me a diskette called 'Charlie'. This virus turned out to be what everyone else eventually called the 'Vienna' virus, and it was the first virus I'd seen that infected files. Swoboda has since become one of the international community of virus researchers, but at that time we both felt very alone.

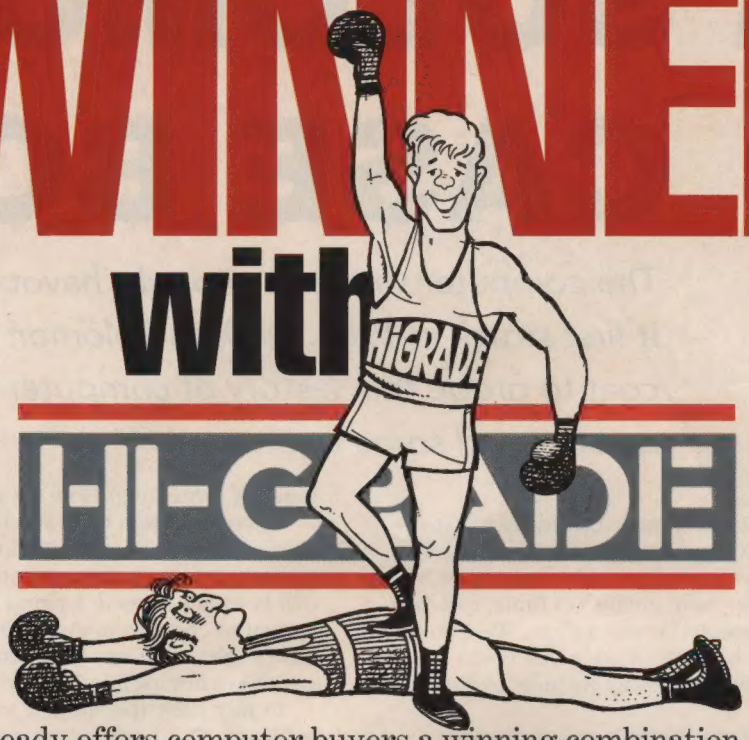
In those days, many people thought the only way to find out what a virus did was through trial and error. You gave the virus interesting dates and files, and observed what it did. The trouble was you ran the risk of never stumbling on the circumstances the virus is looking for.

But there is another method; disassembly. You convert the virus's binary code to assembler language instructions using a suitable program (Debug is one of the best for this). You then work out what the code is doing, block by block. Disassembly, analysis and understanding tells you what the virus does.

Finally, you make sure you understand the code by running the virus under the necessary conditions and then check you were correct. There's nothing magic about this technique; it was taught in schools 25 years ago. It's called the 'Scientific Method', and has been working well for hundreds of years.

The final element of the 'Scientific Method' is the publication of the results. When they are published it's

Be a WINNER with HI-GRADE



Hi-Grade already offers computer buyers a winning combination of top quality hardware, friendly and reliable service and maximum value for money. One reason we can do so is that we sell direct to end users.

To improve that winning formula we plan to put even more effort into studying, and catering for, users' needs. That is why we are starting a Hi-Grade Club. Members will receive a range of benefits, including special discounts and bonuses (on top of our normal attractive prices) and advance news of upgrades and new products and services.

Joining the Club costs nothing. Send for an entry form, which includes a simple questionnaire about who you are and the use you make, or intend to make, of computers.

Filling in that form will give you a chance of becoming a winner in another sense. The names of all Club members will be entered in a draw to be held in December 1991.

First prize: a Hi-Note

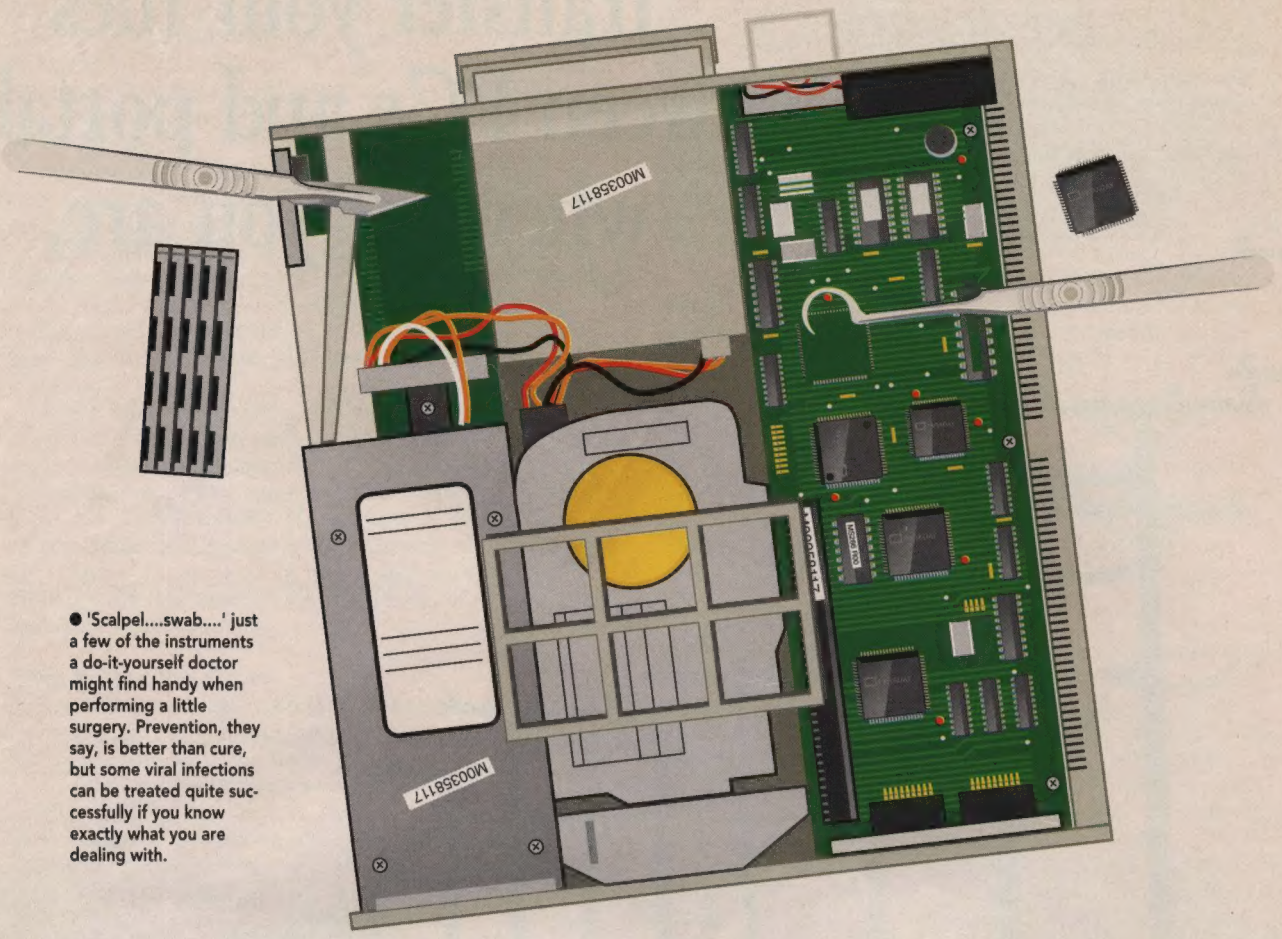
The Hi-Note is Hi-Grade's notebook computer, and a splendid little creature it is. It has a 386SX processor and a high resolution LCD backlit display screen, runs at 20MHz and weighs only 5.9lbs, including battery.
So back the winning side.
Send for a brochure and a Club membership form today.
After all, you've got absolutely nothing to lose.
Not even the price of a stamp.

HI-GRADE
COMPUTERS

Unit 1, Cromwell Centre, 32 Thames Rd, Barking, Essex IG11 0HZ.
Phone 081 591 9040. Fax 081 591 1586
Central London Branch: Phone 071 482 4024
Scottish Branch: Phone 0899 21315

To Hi-Grade Computers Ltd, FREEPOST, Barking, Essex IG11 0BR
Please send me a brochure and a Club membership form

Name_____ Company_____ Address_____ Position_____



● 'Scalpel....swab....' just a few of the instruments a do-it-yourself doctor might find handy when performing a little surgery. Prevention, they say, is better than cure, but some viral infections can be treated quite successfully if you know exactly what you are dealing with.

possible for other researchers to check your work.

If you're unlucky, they'll find mistakes and disagree with you. This doesn't happen as a rule, and any report is summarised by several plagiarists, and passed on as their own work. There must be an authoritative source of information that has been checked independently, and in which any mistakes are corrected promptly. The University of Hamburg is working on such a project.

New Viruses

In August 1988, someone contacted me to say that the letters were falling from his screen and gathering at the bottom. This turned out to be the 'Cascade' virus, and it was the first memory-resident file virus. The memory-resident technique makes for a more infectious virus, and this virus was variably encrypted – the first such virus.

In November 1988 we had a call from Spain. 'There's something spreading all over my hard disk, could you help me?' the customer queried. He sent us some files to analyse, and we found the problem to be the 'Jerusalem' virus. This was the first virus that could infect EXE as well as COM files, and it is now as prevalent as 'Stoned'.

The next step was our first seminar on viruses in December 1988. We hoped that at least a dozen people would attend, but when over 100 people turned up we had to hire a cinema. Clearly, this had become a very interesting subject.

During that month, we also had to do the first big virus clean-up. A major financial institution in the City had the 'Jerusalem' virus. We never traced how it had come in, but it was in the PC Support department, and they had unwittingly spread it quite far. We planned to check every floppy and hard disk, using a scanning program that I wrote for the purpose. There were several hundred computers, and it looked like a big job.

We were helped by many of my own staff, and the job was finished several days later. But it was clear that we couldn't get involved in very many operations like that.

Software Development

Over the next three months, we wrote the first *Anti-Virus Toolkit*. We wanted tools that would allow anyone to do everything necessary with viruses. The first version detected six viruses, and we announced that upgrades would accompany any new viruses. There certainly were new ones, and one of the most striking was the 'Datacrime' virus.

Hysteria Breaks Out

In May 1989, a desperate customer phoned to plead; 'I've found this thing all over my hard disk; can you help me?'. He sent us a file, and on analysis we found that after 12 October (13 October to 31 December) it triggers a low level format of cylinder zero of your hard disk. This infects your partition and boot sector and much of your FAT (File Allocation Table), depending on your disk geometry. This was the first virus that was unambiguously aiming to do damage, so we wrote it up. After triggering, it announced its name – 'Datacrime'.

The report was reprinted in the press, and rumours about a new virus, the 'Columbus Day', were rife in the US. None of our US contacts had a copy, but they were anxious to look at 'Datacrime' in case it spread over there. So we sent them a specimen.

Soon, 'Columbus Day' arrived from the US. On examination it turned out to be 'Datacrime', so we looked up

Transfer your files between PCs and portables wherever you are.

LapLink has always been the easiest way to transfer files between two PCs.

But now, with its new modem transfer capability, it's just as simple to copy files to any computer in the world. All you need is a Hayes compatible modem and access to a phone connection.

LapLink Pro can even install itself onto the target PC over the modem link or serial cable.

On screen you'll find pull-down menus, allowing you to use mouse, keyboard or hot-keys.

LapLink Pro is intelligent at determining which ports are in use and automatically displays all available port connections. And using new data communication and compression technologies, LapLink Pro increases data transfer rates using the serial and parallel cables by up to 20%. File transfer using modems is up to 60% faster than other communication software packages.

You can even edit files prior to transferring them, using the LapLink Editor.

Finally, we've also improved our cables. The new TraveLite serial cable is lighter, thinner and longer (2.4 metres). After all, when you're on the road, the less weight the better.

LapLink Pro comes complete with both serial and parallel cables and cable carrying-case for £125 + VAT.

All you need is LapLink Pro and you'll be ready to transfer files, wherever you may be.

Call us on 0734 321154/ 321099 today for more information or the name of your nearest dealer.

LAPLINK PRO

TRAVELING SOFTWARE

the date of Columbus Day in my diary, and it was 12 October. Clearly there was a confusion about dates; 'Datacrime' goes off on any day after 12 October, not on that date. By this time confusion had been compounded, and there were reports of a virus that went off on the 12 October and reports of yet another one that went off on the 13 October.

Reports began appearing, stating that the 'Columbus Day' virus was written by Norwegian terrorists, upset that Eric the Red, not Columbus, discovered America.

Meanwhile, hysteria was building up in Europe. The Dutch police decided a crime was involved, and that they ought to get involved in the software business. So they commissioned a programmer to write a scanner, which they then offered via the police stations for three guilders (about £1).

When the police started taking it seriously, so did everyone else. Long queues developed outside the police stations. After a few days, the Dutch police found that selling disks for three guilders doesn't relieve you of the technical support burden. People started calling them asking 'What do I do now?' Unfortunately, the software also flagged some innocent files as infected, and they were getting false alarms. They recalled the software and issued version two.

Calm Before the Storm

Meanwhile, it was discovered that 'Datacrime' had a very feeble replication method, and although we had a detector for it in the field, we were getting no reports of it. We spread the word that this was a very rare virus.

But panic had set in. IBM customers started calling their salesman to ask what the company was doing to help with the 'Datacrime' problem. IBM worked against the 13 October deadline, and decided to release 'Virscan', its internal-use-only virus scanner.

This was sent out to important customers, with a disk and a letter explaining how to use it. A lot of hard disks were scanned in the run up to 13 October.

The classic six viruses were found; 'Brain', 'Italian', 'Stoned', 'Cascade', 'Jerusalem' and 'Vienna', but not 'Datacrime'. On 13 October, the hysteria had reached fever pitch, and a few viruses were found, especially Jerusalem (on Friday 13, each program that is run is deleted instead).

Reports were rife that the RNIB (Royal National Institute for the Blind) had an outbreak that led to the loss of six month's research and hundreds of thousands of pounds worth of data.

By the Saturday everything had calmed down a bit, and they phoned us. On the Monday we found the problem to be a minor outbreak of 'Jerusalem', with a few programs deleted (easily re-installed) and no data loss. It took us 30 minutes to get things back to normal. We donated a large amount of anti-virus software to them and that was that.

'Datacrime' was probably on one or two computers in the whole world; the media created the impression that it was everywhere. There were three main consequences of the 'Datacrime' story. Firstly, many people took it seriously because of the reactions of the Dutch police and IBM. Secondly the fuss, followed by silence, caused people to believe that the virus problem all happened in 1989, and has now gone away. Finally, many people who used scanners for the first time decided to continue.

Virus Growth

There were only about 30 viruses by the end of 1989. But by the end of 1990, this had mushroomed out to in the region of 150. But by the end of 1991, there will probably be as many as 1,000, since there were 800 at the end of September 1990 and the tally will go on rising.

As the number of viruses grows, so does their complexity. Some viruses can't be detected with a constant search string. For example, the longest constant search string you can find in Maltese, 'Amoeba', is two bytes long. That's no use as a search string, as every hard disk would have at least one file that had that pair of bytes in it somewhere.

Virus researchers have had to develop new ways to detect this sort of virus. It has also made it difficult for developers of anti-virus software, who rely on published search strings. We spoke to one who had decided he would not detect any virus that did this kind of thing.

The Battle Ground

The virus authors also aim to defeat checksummers. For example, if a file infected with the 'Frodo' virus, is read by a program, it will only allow the program to see the bytes that were in the file before the virus infected it. This makes it impossible for a checksummer to detect the change that it relies on. Users of such software should do a power-off boot from a clean DOS diskette. But it is almost impossible to persuade people to do this.

Another development is the VX (Virus Exchange) bulletin boards (BBS). These allow people to upload and download viruses. There's one in Bulgaria, one in Italy, one in Sweden, one in the US, and four in Britain. Of the British BBSs, two are run by known virus researchers, and the other two are not. One of these has an area for virus development; download binaries and source code, and upload the changed and new viruses.

It seems this is not a criminal activity; for the police have not arrested anyone, even though names and addresses are known. It's difficult to see how to persuade a virus bulletin board system operator who is involved in this sort of thing that what he's doing is wrong and to make him stop.

Plans for the Future

There are a few hopeful signs for the future. Recently, the European Institute for Computer Antivirus Research (EICAR) was formed. One of the first things to come out of the new organisation is a standard for virus names. This will, hopefully, end the confusion whereby every vendor chooses a different virus name, and it's not possible to compare products.

EICAR is a European solution to an essentially European problem. There are few viruses coming from America. Eastern Europe (especially Bulgaria), Russia, Germany, Austria, Switzerland, Italy and France are the main virus-writing countries, although there are a few that come from the UK, most of them with exotic and unlikely sounding names such as Fu Manchu, Green Caterpillar and Jabberwocky.

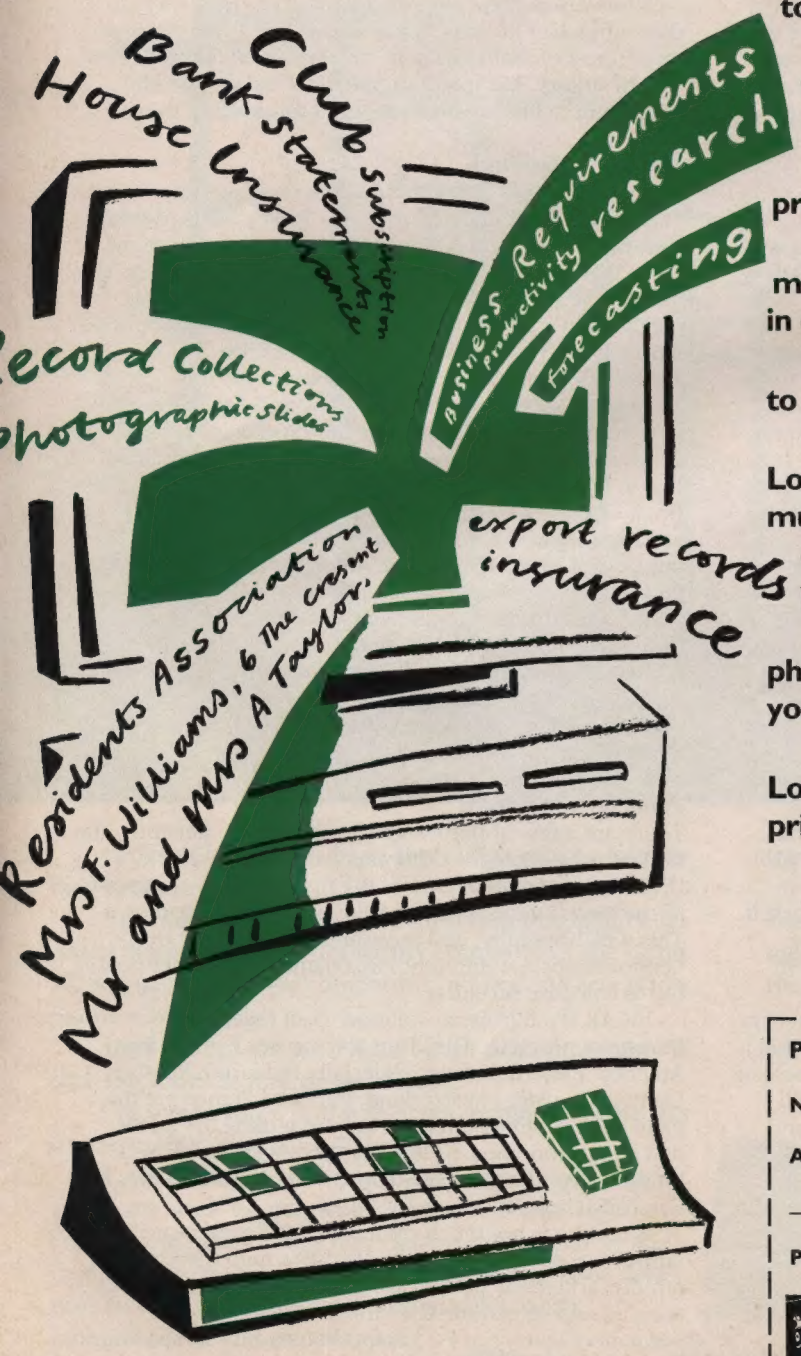
But there is not much optimism. More and more viruses are being written, the VX BBSs help them spread rapidly, and many people are taking little or no precautions against infection. The virus problem is now a permanent feature of PC computing, and its dangers must be taken into consideration by anyone who operates a computer as a matter of routine. ●

ESSENTIAL TIPS

PC users concerned with avoiding viruses need follow one golden rule; when your anti-virus software detects a virus, don't panic, just call your normal support person.

For PC Support staff, the rule is equally simple; when you find a virus, don't panic but read your manual and do exactly what it recommends.

LocoScript PC. Simply the easiest word processing software you can lay your hands on.



LocoScript has become the UK's best selling word processing software for the simple reason that it's really easy to use. Even if you've never touched a computer before.

Well it's now available for the PC, with all the features you'd expect of PC software.

Like split screen editing, phonetic spelling correction and support for virtually every printer available.

You also get a fully integrated database, plus mail merge for mailshots and reports. Documents in every European language, too.

Yet, unlike other PC software, it's very easy to use.

If you use an Amstrad PCW, you'll find LocoScript PC works in just the same way but is much faster. Add LocoLink and all your PCW documents can easily be transferred directly to your PC.

To find out more, just fill in the coupon or phone Jane Anders on (0306) 740606 for details of your nearest authorised dealer.

You'll discover that word processing with LocoScript PC gives you everything you need at a price you can afford.

LocoScript

Please send me more information on LocoScript PC JA

Name _____

Address _____

_____

Postcode _____ Tel: _____

LOCOMOTIVE SOFTWARE

Dorking Business Park, Dorking, Surrey RH4 1YL

EVERYTHING YOU NEED. NOTHING YOU DON'T.

LocoScript PC costs £125 and LocoLink costs £29.95. Prices exclude VAT. Locomotive Software, Dorking, Surrey RH4 1YL